



Centers for Medicare & Medicaid Services

# **CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role**

---

March 30, 2016  
Version 1.0 Final

## Table of Contents

1.	Introduction	2
2.	Step-by-Step Instructions to Register for Multi-Factor Authentication (MFA) in CMS.gov Enterprise Portal	3
3.	Remove a Registered Multi-Factor Authentication (MFA) Device	14
4.	Login Using MFA	19

## 1. Introduction

This guide provides step-by-step instructions on how users who already have an active CMS.gov Enterprise Portal account and a role in <***Your Application Name***> can register for Multi-Factor Authentication (MFA), remove a registered MFA device, and log in with MFA.

**Note:** Do not use this guide if you do not have a role in <***Your Application Name***>. If you want to request a role in <***Your Application Name***>, please refer to the 'EIDM Quick Reference Guide for New Users Completing RIDP and MFA'. If you do not have an EIDM account and want to register for one, visit <https://portal.cms.gov>.

## 2. Step-by-Step Instructions to Register for Multi-Factor Authentication (MFA) in CMS.gov Enterprise Portal

### MFA

MFA is a security mechanism that is implemented to verify the legitimacy of a person or transaction.

MFA requires you to provide more than one form of verification in order to prove your identity. MFA registration is required only once when you are requesting a role, but will be verified every time you log into the CMS Enterprise Portal.

During the MFA registration process, the CMS.gov Enterprise Portal requires registration of a phone, computer, or email to add an additional level of security to a user's account.

You may select from the following options to complete the registration process:

- **Smart Phone:** Download Verification and Identity Protection (VIP) access software on your smart phone/tablet. You must enter the alphanumeric credential ID that is generated by the VIP access client. You will then enter the Security Code generated by the VIP client.
- **Computer:** Download VIP access software on your computer. You must enter the alphanumeric credential ID generated by the VIP access client. You will enter the Security Code generated by the VIP client.
- **E-mail:** Select the e-mail option to receive an e-mail containing a Security Code required at login. You must provide a valid, accessible e-mail address.
- **Short Message Service (SMS):** Use the SMS option to have your Security Code texted to your phone. You must enter a valid phone number. The phone must be capable of receiving text messages. Carrier charges may apply.
- **Interactive Voice Response (IVR):** Select the IVR option to receive a voice message containing your Security Code. You must provide a valid phone number and (optional) phone extension.

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

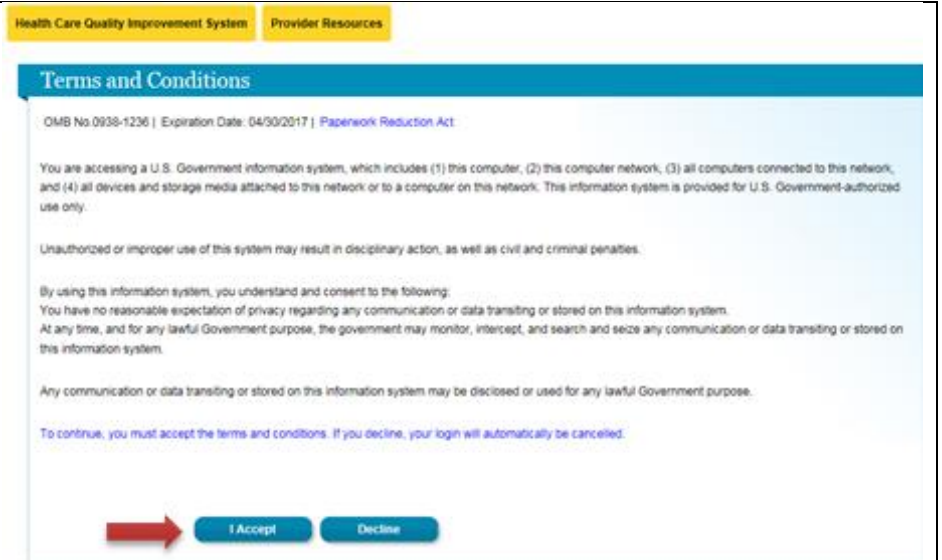
## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the <b>CMS Enterprise Portal</b>.</p> <p><b>Note:</b> The CMS Enterprise Portal supports the following internet browsers:</p> <ul style="list-style-type: none"><li>• Internet Explorer 8, 9, 10, and 11</li><li>• Mozilla-Firefox</li><li>• Chrome</li><li>• Safari</li></ul>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

2. Read the Terms and Conditions and select **I Accept** to continue.



Health Care Quality Improvement System Provider Resources

### Terms and Conditions

OMB No.0938-1236 | Expiration Date: 04/30/2017 | [Paperwork Reduction Act](#)

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

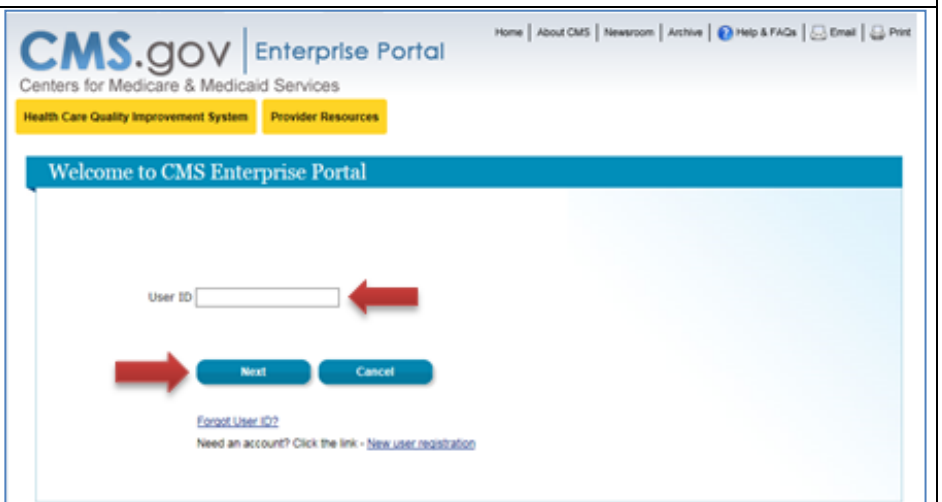
By using this information system, you understand and consent to the following:  
You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system.  
At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

To continue, you must accept the terms and conditions. If you decline, your login will automatically be canceled.

**I Accept** Decline

3. Enter your **User ID** and select **Next**.



CMS.gov Enterprise Portal  
Centers for Medicare & Medicaid Services

Health Care Quality Improvement System Provider Resources

### Welcome to CMS Enterprise Portal

User ID

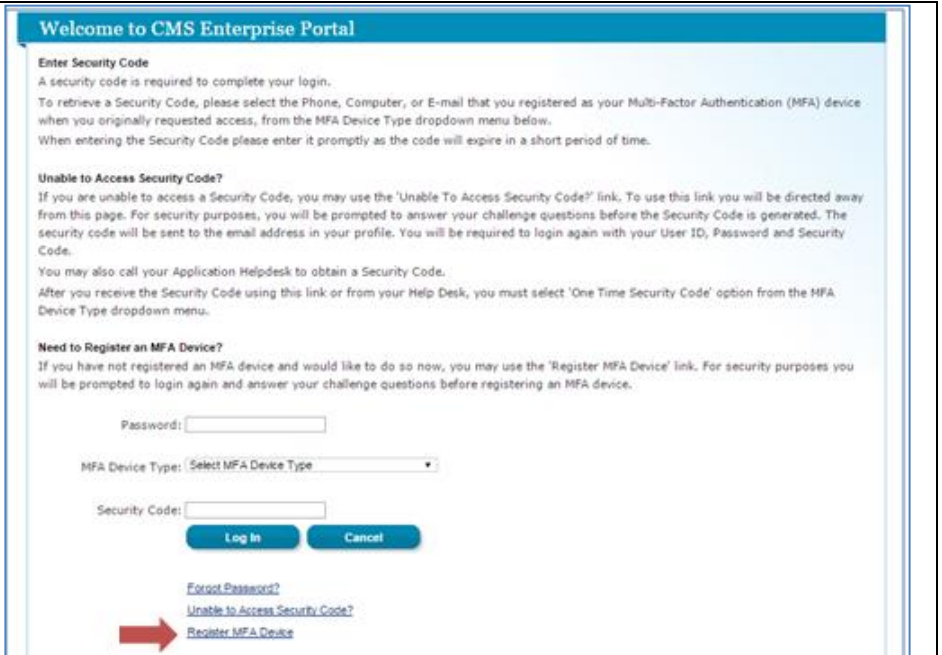
**Next** Cancel

[Forgot User ID?](#)  
Need an account? Click the link - [New user registration](#)

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

### 4. Select the **Register MFA Device** link.



**Welcome to CMS Enterprise Portal**

**Enter Security Code**  
A security code is required to complete your login.  
To retrieve a Security Code, please select the Phone, Computer, or E-mail that you registered as your Multi-Factor Authentication (MFA) device when you originally requested access, from the MFA Device Type dropdown menu below.  
When entering the Security Code please enter it promptly as the code will expire in a short period of time.

**Unable to Access Security Code?**  
If you are unable to access a Security Code, you may use the 'Unable To Access Security Code?' link. To use this link you will be directed away from this page. For security purposes, you will be prompted to answer your challenge questions before the Security Code is generated. The security code will be sent to the email address in your profile. You will be required to login again with your User ID, Password and Security Code.  
You may also call your Application Helpdesk to obtain a Security Code.  
After you receive the Security Code using this link or from your Help Desk, you must select 'One Time Security Code' option from the MFA Device Type dropdown menu.

**Need to Register an MFA Device?**  
If you have not registered an MFA device and would like to do so now, you may use the 'Register MFA Device' link. For security purposes you will be prompted to login again and answer your challenge questions before registering an MFA device.

Password:

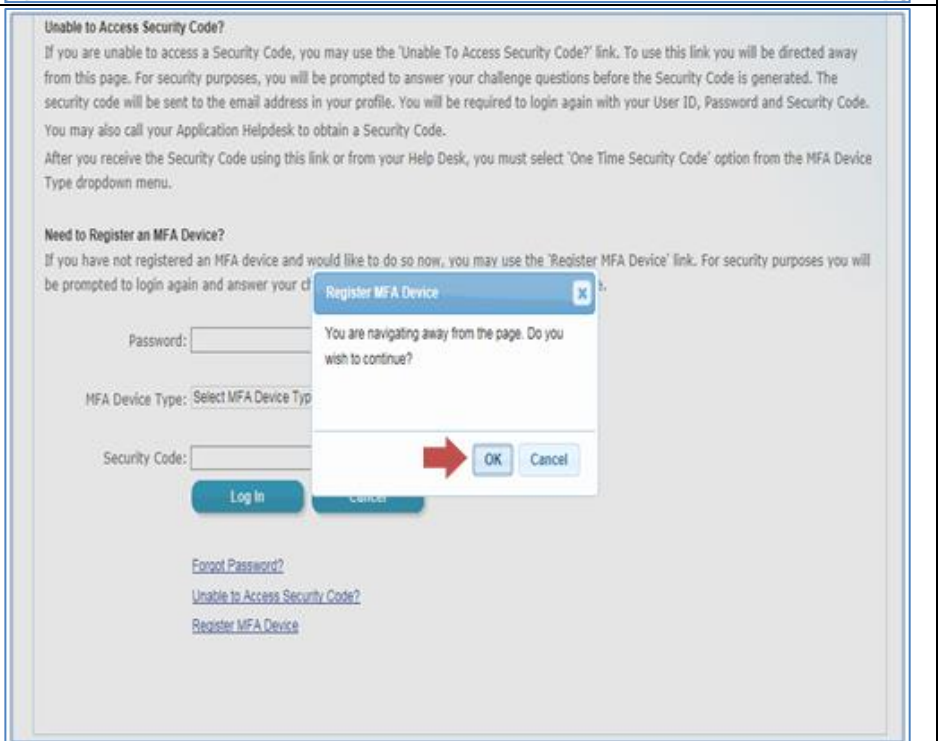
MFA Device Type:

Security Code:

[Forgot Password?](#)  
[Unable to Access Security Code?](#)  
[Register MFA Device](#)

### 5. Select **OK** to navigate away from the login page.

**Note:** Selecting **Cancel** will end the process to register an MFA Device.



**Unable to Access Security Code?**  
If you are unable to access a Security Code, you may use the 'Unable To Access Security Code?' link. To use this link you will be directed away from this page. For security purposes, you will be prompted to answer your challenge questions before the Security Code is generated. The security code will be sent to the email address in your profile. You will be required to login again with your User ID, Password and Security Code.  
You may also call your Application Helpdesk to obtain a Security Code.  
After you receive the Security Code using this link or from your Help Desk, you must select 'One Time Security Code' option from the MFA Device Type dropdown menu.

**Need to Register an MFA Device?**  
If you have not registered an MFA device and would like to do so now, you may use the 'Register MFA Device' link. For security purposes you will be prompted to login again and answer your challenge questions before registering an MFA device.

Password:

MFA Device Type:

Security Code:

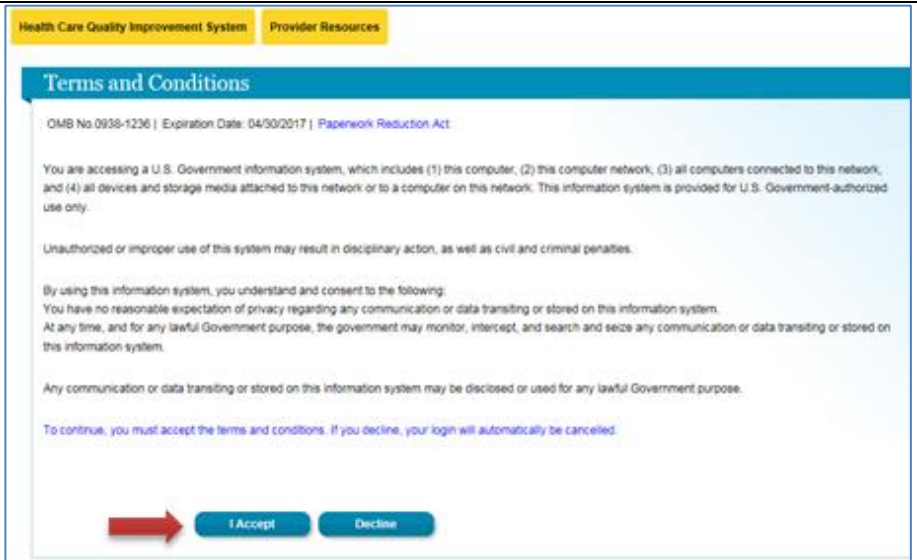
[Forgot Password?](#)  
[Unable to Access Security Code?](#)  
[Register MFA Device](#)

**Register MFA Device**  
You are navigating away from the page. Do you wish to continue?

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

6. Read the Terms and Conditions and select **I Accept**.



Health Care Quality Improvement System | Provider Resources

### Terms and Conditions

OMB No 0938-1236 | Expiration Date: 04/30/2017 | [Paperwork Reduction Act](#)

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.


By using this information system, you understand and consent to the following:

You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system.

At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

To continue, you must accept the terms and conditions. If you decline, your login will automatically be cancelled.



7. Enter your **User ID** and **Password**, and select **Log In**.



CMS.gov | Enterprise Portal  
Centers for Medicare & Medicaid Services

Home | About CMS | Newsroom | Archive | [Help & FAQs](#) | [Email](#) | [Print](#)

Health Care Quality Improvement System | Provider Resources

### Welcome to CMS Enterprise Portal

 User ID:

 Password:



[Forgot Password?](#)  
[Forgot User ID?](#)  
Need an account? Click the link - [New user registration](#)

If you have questions or need assistance regarding MFA, please contact your Application Help Desk



## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

8. Answer the challenge questions and select **Next**.

The screenshot shows the 'Register MFA Device' page on the CMS.gov Enterprise Portal. It includes a 'My Portal' button, a breadcrumb 'CMS Portal > Register MFA Device', and links for 'Screen reader mode Off' and 'Accessibility Settings'. The main heading is 'Please answer the following challenge questions'. There are three text input fields with red arrows pointing to them from the right: 'What is the name of your favorite pet?', 'What was your favorite toy when you were a child?', and 'What is your favorite radio station?'. Below the fields are 'Cancel' and 'Next' buttons, with a red arrow pointing to the 'Next' button. At the bottom, there is a note about login issues and a link to the 'Enterprise User Administration (EUA) page'.

9. Select an MFA device from the **MFA Device Type** dropdown.

**Note:** You can select the arrows on the left of each MFA Device Type for additional information.

The screenshot shows the 'Register MFA Device' page on the CMS.gov Enterprise Portal. It includes a 'My Portal' button, a breadcrumb 'CMS Portal > Register MFA Device', and links for 'Screen reader mode Off' and 'Accessibility Settings'. The main heading is 'Registered MFA Devices'. Below this, it says 'There are no MFA devices associated with your profile.' The next section is 'Register Your Phone, Computer, or E-mail'. It contains a paragraph about adding a security code and a list of links: '> Phone/Tablet/PC/Laptop', '> Text Message Short Message Service (SMS)', '> Interactive Voice Response (IVR)', and '> E-mail'. Below the links is a note about two attempts. At the bottom, there is a dropdown menu labeled 'MFA Device Type: Select MFA Device Type' with a red arrow pointing to it. Below the dropdown are 'Cancel' and 'Next' buttons.

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

9(a). If selecting **Phone/Tablet/PC/Laptop** as the **MFA Device Type**, enter the alphanumeric code that displays under the field labeled Credential ID (on the VIP Access software) in the **Credential ID** field. Enter a brief description (e.g., Laptop) in the field labeled **MFA Device Description**. Then select **Next**.

### MFA Option (a) Screenshots

#### Register Your Phone, Computer, or E-mail

Adding a Security Code to your login also known as Multi-Factor Authentication (MFA) can make your login more secure by providing an extra layer of protection to your user name and password.

You can associate the Security Code to your profile by registering your phone, computer or E-mail. Select the links below to find out more information about the options.

##### Phone/Tablet/PC/Laptop

To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -<https://m.vip.symantec.com/home.v>

To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -<https://idprotect.vip.symantec.com/desktop/download.v>

##### Text Message Short Message Service (SMS)

The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.

##### Interactive Voice Response (IVR)

The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. The option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks\*, period., comma., pound # followed by numeric 0 to 9. For example 4895554444, 1112.

To access the application you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.

##### E-mail

The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail option. When logging into a secure application, your Security Code that is required at the login page will be e-mailed to the e-mail address on the profile.

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.

MFA Device Type: Phone/Tablet/PC/Laptop

Enter the alphanumeric code that displays under the label Credential ID on your device.

Credential ID: VSST63534857

MFA Device Description: PC Option

Cancel

Next



If you have questions or need assistance regarding MFA, please contact your Application Help Desk

OR

9(b). If selecting **Text Message – Short Message Service (SMS)** as the **MFA Device Type**, enter the **Phone Number** that will be used to obtain the Security Code. Enter a brief description (e.g., Text) in the field labeled **MFA Device Description** and select **Next**.

OR

### MFA Option (b) Screenshot

#### Register Your Phone, Computer, or E-mail

Adding a Security Code to your login also known as Multi-Factor Authentication (MFA) can make your login more secure by providing an extra layer of protection to your user name and password.

You can associate the Security Code to your profile by registering your phone, computer or E-mail. Select the links below to find out more information about the options.

##### Phone/Tablet/PC/Laptop

To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -<https://m.vip.symantec.com/home.v>

To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -<https://idprotect.vip.symantec.com/desktop/download.v>

##### Text Message Short Message Service (SMS)

The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.

##### Interactive Voice Response (IVR)

The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. The option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks\*; period.; comma.; pound # followed by numeric 0 to 9. For example: 4885554444, 1112.

To access the application you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.

##### E-mail

The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail option. When logging into a secure application, your Security Code that is required at the login page will be e-mailed to the e-mail address on the profile.

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.

MFA Device Type: Text Message-Short Message Service (SMS) 

Enter the phone number that will be used to obtain the Security Code.

Phone Number: 111 222 3333 

MFA Device Description: Text 

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

OR

9(c). If selecting **Voice Message – Interactive Voice Response (IVR)** as the **MFA Device Type**, enter the **Phone Number** and corresponding **Extension** that will be used to obtain the Security Code. Enter a brief description (e.g., IVR) in the field labeled **MFA Device Description** and select **Next**.

**Note:** *Extension is an optional field. You may choose to provide a 10-digit phone number or a phone number with an extension.*

OR

### MFA Option (c) Screenshot

Register Your Phone, Computer, or E-mail

Adding a Security Code to your login also known as Multi-Factor Authentication (MFA) can make your login more secure by providing an extra layer of protection to your user name and password.

You can associate the Security Code to your profile by registering your phone, computer or E-mail. Select the links below to find out more information about the options.

▽ Phone/Tablet/PC/Laptop

To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -<https://m.vip.symantec.com/home.v>

To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -<https://idprotect.vip.symantec.com/desktop/download.v>

▽ Text Message Short Message Service (SMS)

The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.

▽ Interactive Voice Response (IVR)

The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. The option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks '\*'; period '.'; comma ','; pound '#' followed by numeric 0 to 9. For example: 4895554444, 1112.


To access the application you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.

▽ E-mail

The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail option. When logging into a secure application, your Security Code that is required at the login page will be e-mailed to the e-mail address on the profile.

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.

• MFA Device Type:  

Enter the phone number that will be used to obtain the Security Code.

• Phone Number:    Extension:  

• MFA Device Description:  



If you have questions or need assistance regarding MFA, please contact your Application Help Desk

OR

9(d). If selecting **E-mail** as the **MFA Device Type**, the E-mail address on your profile will be automatically used to obtain the Security Code. Enter a brief description (e.g., E-mail) in the field labeled **MFA Device Description** and select **Next**.

**Note:** The E-mail address cannot be changed at the time of MFA device registration. It can only be changed using the 'Change E-Mail Address' option from the 'Change My Profile' menu.

OR

### MFA Option (d) Screenshot

Register Your Phone, Computer, or E-mail

Adding a Security Code to your login also known as Multi-Factor Authentication (MFA) can make your login more secure by providing an extra layer of protection to your user name and password.

You can associate the Security Code to your profile by registering your phone, computer or E-mail. Select the links below to find out more information about the options.

- ▼ **Phone/Tablet/PC/Laptop**  
To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -<https://m.vip.symantec.com/home.v>  
To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -<https://idprotect.vip.symantec.com/desktop/download.v>
- ▼ **Text Message Short Message Service (SMS)**  
The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.
- ▼ **Interactive Voice Response (IVR)**  
The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. The option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks "\*", period "."; comma ","; pound "W" followed by numeric 0 to 9. For example: 4885554444, 1112.  
To access the application you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.
- ▼ **E-mail**  
The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail option. When logging into a secure application, your Security Code that is required at the login page will be e-mailed to the e-mail address on the profile.  
Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.

MFA Device Type: E-mail ▼

E-mail Address:

The E-mail address on your profile will automatically be used for the E-mail option. Your e-mail address cannot be changed at the time of MFA registration. To change your E-mail please select 'Change E-Mail Address' from the 'Change My Profile' menu.

MFA Device Description:

10. Your registration for the **Multi-Factor Authentication** is now complete. Select **OK** to continue to log in with MFA.

**Note:** You will receive an E-mail notification for successfully registering the MFA Device Type.

CMS.gov Enterprise Portal  
Centers for Medicare & Medicaid Services  
Health Care Quality Improvement System Provider Resources  
CMS Portal > Register MFA Device  
Screen reader mode Off | Accessibility Settings

**Register Your Phone, Computer, or E-mail**

You have successfully registered your Phone/Computer/E-mail to your user profile.

Click "OK" to close this window and login.

If you have questions or need assistance regarding MFA, please contact your Application Help Desk



11. Enter your **User ID** and select **Next** to continue to log in.

CMS.gov | Enterprise Portal  
Centers for Medicare & Medicaid Services

Health Care Quality Improvement System Provider Resources

Welcome to CMS Enterprise Portal

User ID

Next Cancel

[Forgot User ID?](#)  
Need an account? Click the link - [New user registration](#)

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

### 3. Remove a Registered Multi-Factor Authentication (MFA) Device

To remove a registered Phone or Computer, please follow each step listed below unless otherwise noted.

Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the <b>CMS Enterprise Portal</b>.</p> <p><b>Note:</b> The CMS Enterprise Portal supports the following internet browsers:</p> <ul style="list-style-type: none"><li>• Internet Explorer 8, 9, 10, and 11</li><li>• Mozilla-Firefox</li><li>• Chrome</li><li>• Safari</li></ul>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

2. Read the Terms and Conditions and select **I Accept** to continue.

Health Care Quality Improvement System Provider Resources

### Terms and Conditions

OMB No.0938-1236 | Expiration Date: 04/30/2017 | [Paperwork Reduction Act](#)

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:  
You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system.  
At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

To continue, you must accept the terms and conditions. If you decline, your login will automatically be cancelled.

**I Accept** Decline

3. Enter your **User ID** and select **Next** to continue.

CMS.gov Enterprise Portal  
Centers for Medicare & Medicaid Services

Home | About CMS | Newsroom | Archive | Help & FAQs | Email | Print

Health Care Quality Improvement System Provider Resources

### Welcome to CMS Enterprise Portal

User ID

**Next** Cancel

[Forgot User ID?](#)  
Need an account? Click the link - [New user registration](#)

If you have questions or need assistance regarding MFA, please contact your Application Help Desk



## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

4. Enter your **Password**, select an MFA device from the **MFA Device Type** dropdown, and select **Log In**.

**Note:** You should select the **MFA Device Type** that you previously registered.

**Welcome to CMS Enterprise Portal**

**Enter Security Code**  
A security code is required to complete your login.  
To retrieve a Security Code, please select the Phone, Computer, or E-mail that you registered as your Multi-Factor Authentication (MFA) device when you originally requested access, from the MFA Device Type dropdown menu below.  
When entering the Security Code please enter it promptly as the code will expire in a short period of time.

**Unable to Access Security Code?**  
If you are unable to access a Security Code, you may use the 'Unable To Access Security Code?' link. To use this link you will be directed away from this page. For security purposes, you will be prompted to answer your challenge questions before the Security Code is generated. The security code will be sent to the email address in your profile. You will be required to login again with your User ID, Password and Security Code.  
You may also call your Application Helpdesk to obtain a Security Code.  
After you receive the Security Code using this link or from your Help Desk, you must select 'One Time Security Code' option from the MFA Device Type dropdown menu.

**Need to Register an MFA Device?**  
If you have not registered an MFA device and would like to do so now, you may use the 'Register MFA Device' link. For security purposes you will be prompted to login again and answer your challenge questions before registering an MFA device.

→ Password:

→ MFA Device Type:

→ Security Code:

→

[Forgot Password?](#)  
[Unable to Access Security Code?](#)  
[Register MFA Device](#)

5. Select your username and then select **My Profile** from the dropdown menu to go to your profile.

Portal Help & FAQs Print Log Out Welcome smoke cranabi

**CMS.gov Enterprise Portal**

My Portal

CMS Portal > EOL user menu page > My Access

**Access Catalog** Start typing to filter apps. REQUEST ADMIN ROLE SHOW ALL

**My Access**

HPG  
Help Desk Information: 800-324-7215  
[hp@cms.gov](mailto:hp@cms.gov)  
Existing Roles: MOORE HPG Desk

**My Pending Requests**  
You do not have any pending requests at this time.

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

6. Select the **Remove Your Phone, Computer, or E-mail** link to remove a registered MFA device from your profile.

Select the radio button next to the device you wish to remove, enter the **Security Code** sent to your device, and select **Next** to continue.

CMS.gov Enterprise Portal

My Portal ELMO ▼

CMS Portal > EIDM user menu page > My Profile

Screen reader mode Off | Accessibility Settings

Change My Profile  
View My Profile  
Change Password  
Register Your Phone, Computer, or E-mail  
Remove Your Phone, Computer, or E-mail

View My Profile

First Name : sally  
Last Name : smith  
Date of Birth : 02/02/1990  
E-mail Address : chjohnson@qssinc.com

U.S. Home Address

Phone Number : 2406669999  
Home Address Line 1 : 321 sandy road  
Home Address Line 2 :  
City : gaithersburg  
State : MD  
Zip Code : 20879  
Country: USA

7. Select the registered device you want to remove, select **Send Security Code**, enter the security code received on the selected MFA Device Type, and select **Next** to proceed.

**Note:** Selecting **Cancel** will end the device removal process.

Portal Help & FAQs Print Log Out

CMS.gov Enterprise Portal

My Portal HDS FFSOCs ▼

CMS Portal > EIDM user menu page > My Profile

Screen reader mode Off | Accessibility Settings

Change My Profile  
Change E-mail Address  
Change Phone number  
Change Challenge Questions and Answers  
Change Address  
View My Profile  
Change Password  
Register Your Phone, Computer, or E-mail  
Remove Your Phone, Computer, or E-mail

Remove Your Phone, Computer, or E-mail

Credential (or Phone Number/E-mail)	MFA Device Type	MFA Device Description	Remove Selected
17024682434	SMS_OTP	Samara Cell	<input type="radio"/>
17173778104	VOICE_OTP	Shirley Cell	<input type="radio"/>

Enter the security code from a phone or computer that you have already registered with this account. Keep in mind that the Security Code changes every 30 seconds. Please enter and confirm the code promptly.

\* Security Code :

Next Cancel

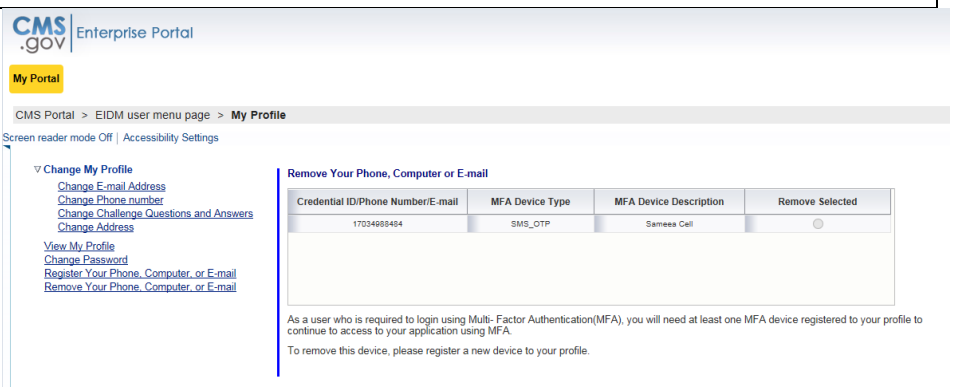
If you have questions or need assistance regarding MFA, please contact your Application Help Desk

8. Removal of your registered MFA device is now complete. Select **OK** to proceed.

**Note:** You will receive an E-mail notification for successfully removing the MFA device.



9. You will need at least one MFA device registered to your profile to continue to access your application using MFA. To remove the last registered device from your profile, you will need to register a new device to your profile.



If you have questions or need assistance regarding MFA, please contact your Application Help Desk

## 4. Login Using MFA

Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the <b>CMS Enterprise Portal</b>.</p> <p><b>Note:</b> The CMS Enterprise Portal supports the following internet browsers:</p> <ul style="list-style-type: none"><li>• Internet Explorer 8, 9, 10, and 11</li><li>• Mozilla-Firefox</li><li>• Chrome</li><li>• Safari</li></ul>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

2. Read the Terms and Conditions and select **I Accept** to continue.

Health Care Quality Improvement System Provider Resources

### Terms and Conditions

OMB No.0938-1236 | Expiration Date: 04/30/2017 | [Paperwork Reduction Act](#)

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:  
You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system.  
At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

To continue, you must accept the terms and conditions. If you decline, your login will automatically be cancelled.

**I Accept** **Decline**

3. Enter your **User ID** and select **Next**.

CMS.gov | Enterprise Portal  
Centers for Medicare & Medicaid Services

Health Care Quality Improvement System Provider Resources

### Welcome to CMS Enterprise Portal

User ID

**Next** **Cancel**

[Forgot User ID?](#)  
Need an account? Click the link - [New user registration](#)

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

4. Enter your **Password**, select an MFA device from the **MFA Device Type** dropdown, and select **Log In**.

**Note:** The Security Code for E-mail and One-Time Security Code will expire in 30 minutes. The Security Code for the other MFA device types will expire in 10 minutes. If you are unable to enter the code within the period, you will need to request a new Security Code.

If you do not have access to your registered MFA device, please refer to the EIDM Quick reference Guide 'EIDM QRG – User Login', for step-by-step instructions on how to register an MFA device.

#### Register Your Phone, Computer, or E-mail

Adding a Security Code to your login also known as Multi-Factor Authentication (MFA) can make your login more secure by providing an extra layer of protection to your user name and password.

You can associate the Security Code to your profile by registering your phone, computer or E-mail. Select the links below to find out more information about the options.

##### Phone/Tablet/PC/Laptop

To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -<https://m.vip.symantec.com/home.v>

To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -<https://idprotect.vip.symantec.com/desktop/download.v>

##### Text Message Short Message Service (SMS)

The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.

##### Interactive Voice Response (IVR)

The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. The option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks "\*", period ".", comma ",", pound "# followed by numeric 0 to 9. For example: 4895554444, 1112.

To access the application you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.

##### E-mail

The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail option. When logging into a secure application, your Security Code that is required at the login page will be e-mailed to the e-mail address on the profile.

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.

MFA Device Type: Phone/Tablet/PC/Laptop

Enter the alphanumeric code that displays under the label Credential ID on your device.

Credential ID: VS5T63534857

MFA Device Description: PC Option

Cancel Next



If you have questions or need assistance regarding MFA, please contact your Application Help Desk



4(a). If you select **Phone/Tablet/PC/Laptop** as the **MFA Device Type**, enter the Security Code that displays under the field labeled Security Code (on the VIP Access software) in the **Security Code** field. Select **Log In**.



Form 4(a) showing the login process for Phone/Tablet/PC/Laptop MFA Device Type.

Password:

MFA Device Type: **Phone/Tablet/PC/Laptop**

The Security Code for the Phone/Tablet/PC/Laptop will expire in 10 minutes.

Security Code:

**Log In** **Cancel**

[Forgot Password?](#)  
[Unable to Access Security Code?](#)  
[Register MFA Device](#)

4(b). If you select **Text Message – Short Message Service (SMS)** or **Interactive Voice Response (IVR)** or **E-mail** as the **MFA Device Type**, select **Send** to receive the Security Code on the selected MFA device type. Enter the Security Code in the **Security Code** field and select **Log In**.

Form 4(b) showing the login process for Interactive Voice Response (IVR) MFA Device Type.

Password:

MFA Device Type: **Interactive Voice Response (IVR)**

The Security Code for the Interactive Voice Response (IVR) will expire in 10 minutes.

**Send**

Security Code:

**Log In** **Cancel**

[Forgot Password?](#)  
[Unable to Access Security Code?](#)  
[Register MFA Device](#)

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

4(c). If you select **One-Time Security Code** as the **MFA Device Type**, enter the Security Code that was sent to your registered E-mail address via the 'Unable to Access Security Code?' link or provided by the Helpdesk, in the **Security Code** field. Select **Log In**.

Password:

➔ MFA Device Type: **One-Time Security Code**

The Security Code for the One-Time Security Code will expire in 30 minutes.

➔ Security Code:

➔ **Log In** Cancel

[Forgot Password?](#)  
[Unable to Access Security Code?](#)  
[Register MFA Device](#)

5. If you are not able to access your Security Code, select the '**Unable to Access Security Code?**' link. On selecting this link, the '**Unable to Access Security Code?**' popup message will be displayed. Select **OK** to continue

Enter Security Code

A security code is required to complete your login.  
To retrieve a Security Code, please select the Phone, Computer, or E-mail that you registered as your Multi-Factor Authentication (MFA) device when you originally requested access, from the MFA Device Type dropdown menu below.  
When entering the Security Code please enter it promptly as the code will expire in a short period of time.

**Unable to Access Security Code?**

If you are unable to access a Security Code, you may use the 'Unable To Access Security Code?' link. To use this link you will be directed away from this page. For security purposes, you will be prompted to answer your challenge questions before the Security Code is generated. The security code will be sent to the email address in your profile. You will be required to login again with your User ID, Password and Security Code.

You may also call your Application Helpdesk to obtain a Security Code.

After you receive the Security Code using this link or from your Help Desk, you must select 'One-Time Security Code' option from the MFA Device Type dropdown menu.

**Need to Register an MFA Device?**

If you have not registered an MFA device and would like to do so now, you may use the 'Register MFA Device' link. For security purposes you will be prompted to login again and answer your challenge questions before registering an MFA device.

Password:

MFA Device Type:

Security Code:

**Log In**

[Forgot Password?](#)  
[Unable to Access Security Code?](#)  
[Register MFA Device](#)

**Unable to Access Security Code**

You are navigating away from the page. Do you wish to continue?

➔ **OK** Cancel

If you have questions or need assistance regarding MFA, please contact your Application Help Desk



## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

6. Enter your **User ID** and select **Next**.

7. Answer the challenge questions and select **Next**.

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

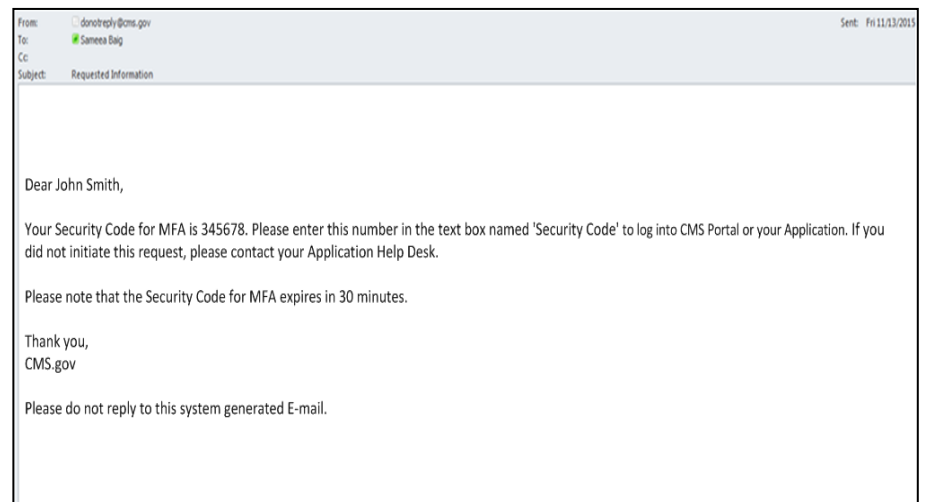
## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

8. Select **OK** to return to the login page.

**Note:** This security code will expire in 30 minutes or after it is used successfully for the first time.



9. An E-mail with the Security Code will be sent to the E-mail address on your profile.



If you have questions or need assistance regarding MFA, please contact your Application Help Desk

## CMS.gov Enterprise Portal Quick Reference Guide for Existing Users Adding Multi-Factor Authentication (MFA) to Application Role

10. Read the Terms and Conditions and select **I Accept** to continue.

Health Care Quality Improvement System Provider Resources

### Terms and Conditions

OMB No.0938-1236 | Expiration Date: 04/30/2017 | [Paperwork Reduction Act](#)

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:  
You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system.  
At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

To continue, you must accept the terms and conditions. If you decline, your login will automatically be cancelled.

[I Accept](#) [Decline](#)

11. Enter your **User ID** and select **Next**.

CMS.gov Enterprise Portal  
Centers for Medicare & Medicaid Services

Health Care Quality Improvement System Provider Resources

### Welcome to CMS Enterprise Portal

User ID

[Next](#) [Cancel](#)

[Forgot User ID?](#)  
Need an account? Click the link - [New user registration](#)

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

12. Enter your **Password**, select **One-Time Security Code** as the **MFA Device Type**, and enter the **Security Code** that was sent to the E-mail address on your profile. Then select **Log In**.

The screenshot shows the 'Welcome to CMS Enterprise Portal' page. It includes instructions for entering a security code and links for password recovery and MFA device registration. Red arrows highlight the login fields: Password, MFA Device Type (set to 'One-Time Security Code'), and the Security Code (345678). The 'Log In' button is also indicated by a red arrow.

Health Care Quality Improvement System | Provider Resources

### Welcome to CMS Enterprise Portal

**Enter Security Code**  
A Security Code is required to complete your login. To retrieve a Security Code, please select the Phone, Computer, or E-mail that you registered as your Multi-Factor Authentication (MFA) device when you originally requested access, from the MFA Device Type dropdown menu below.

When entering the Security Code, please enter it promptly as the code will expire in a short period of time.

**Unable to Access Security Code?**  
If you are unable to access a Security Code, you may use the 'Unable To Access Security Code?' link. To use this link you will be directed away from this page. For security purposes, you will be prompted to answer your challenge questions before the Security Code is generated. The Security Code will be sent to the email address in your profile. You will be required to login again with your User ID, Password and Security Code.

You may also call your Application Help Desk to obtain a Security Code.

After you receive the Security Code using this link or from your Help Desk, you must select the 'One-Time Security Code' option from the MFA Device Type dropdown menu.

**Need to Register an MFA Device?**  
If you have not registered an MFA device and would like to do so now, you may use the 'Register MFA Device' link. For security purposes you will be prompted to login again and answer your challenge questions before registering an MFA device.

Password:

MFA Device Type:

The security code for the Phone/Tablet/PC Laptop will expire in 10 minutes.

Security Code:

[Forgot Password?](#)  
[Unable to Access Security Code?](#)  
[Register MFA Device](#)

If you have questions or need assistance regarding MFA, please contact your Application Help Desk